

- 1. A security modeling system comprising:
  - a network configuration module having network configuration data; and
- a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database.
- 2. The system of claim 1, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.
- 3. The system of claim 2, wherein the network configuration data and the network vulnerability, attack and exploitation data are stored in database tables and the data is processable by a computer.
- 4. The system of claim 1, wherein the network configuration module comprises network configuration data output by a network configuration discovery tool.
- 5. The system of claim 1, wherein the simulator includes a graphical user interface.
- 6. The system of claim 2, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.
- 7. The system of claim 1, wherein the simulator includes a defender and an attacker user interface.
- 8. The system of claim 1, wherein the security modeling system is portable.
- 9. A computer game comprising:a network configuration module having network configuration data;a simulator coupled to the network configuration module for simulating and

5

10

15,

20

10

analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database, and wherein the simulator includes a graphical user interface for playing the game.

- 5 10. A security modeling system comprising:
  - a network configuration module having network configuration data;
  - a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database; and
  - a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information.
  - 11. The system of claim 10, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.
  - 12. The system of claim 11, wherein the network configuration data and the network vulnerability, attack and exploitation data is stored in database tables and the data is processable by a computer.
  - 13. The system of claim 10, wherein the simulator includes a graphical user interface.
  - 14. The system of claim 10, wherein the critical resource information includes goals, expectations and constraints for simulating the network.
- 25 15. The system of claim 10, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.
  - 16. The system of claim 10, wherein the security modeling system is portable.
- The system of claim 10, wherein the simulator includes a defender and an attacker

user interface.

18. A method of analyzing a computer network using a security modeling system, wherein the security modeling system includes a database of network vulnerability information, the method comprising:

providing a network configuration of a computer network; simulating the network based on the network configuration; and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database.

19. The method of claim 18, wherein providing a network configuration includes receiving a configuration as the output of a network discovery tool.

20. The method of claim 18, wherein providing a network configuration includes receiving a data file which includes a configuration of the computer network.

21. The method of claim 18, wherein simulating the network includes: receiving mission objectives; storing the objectives; and simulating the network based on the network configuration and mission objectives.

- 22. The method of claim 21, wherein determining vulnerabilities includes modifying the simulation using a graphical user interface.
- 23. The method of claim 22, wherein modifying the simulation includes dynamically interacting with an attacker.
  - 24. The method of claim 22, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

20

5

10

30

- 25. The method of claim 23, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.
- 26. The method of claim 21, wherein determining vulnerabilities includes computing security results, wherein the security results include a security score.
- 27. The method of claim 21, wherein determining vulnerabilities of the simulated network includes updating the vulnerabilities database when vulnerabilities are detected.
- 28. A method of opposing network attackers comprising:

receiving a network configuration, wherein the network configuration comprises computer hardware and software component information;

receiving mission objectives;

receiving commands from a network attacker;

simulating the network based on the commands received from the network attacker, wherein simulating the network includes determining results as a function of the network configuration, mission objectives and stored vulnerability data for the described computer hardware and software components; and

responding to the network attacker, wherein responding to the attacker includes imposing barriers, providing response messages and protecting the network.

- 29. The method of claim 28, wherein simulating the network further includes receiving commands from a defender and determining results based on the defender commands.
- 25 30. The method of claim 28, wherein receiving configuration includes receiving critical resource information, wherein the critical resource information includes goals, expectation and constraints for simulating the network.
  - 31. The method of claim 28, and further includes modifying the simulation using a graphical user interface.

20

5

- 32. The method of claim 31, wherein determining vulnerabilities includes computing security results which include a security score.
- 33. The method of claim 31, wherein receiving commands includes receiving attack actions which include commands that simulate service functionality, commands that change services or nodes, and commands that exploit vulnerabilities.
- 34. A security modeling system for simulating objective networks comprising:
- a simulator having a plurality of databases, wherein the plurality of databases include mission objectives tables, vulnerability tables, and network configuration tables, wherein the network configuration tables include network configuration data; and
- a graphical user interface which operates with the simulator to allow input and output to clients.
- 35. The system of claim 34, wherein the mission objectives tables include mission tables, mission files tables and mission services tables.
- 36. The system of claim 34, wherein the vulnerability tables include service tables.
- 37. The system of claim 34, wherein the network configuration tables include configuration tables, defense tables, filter tables, node tables, routing tables and password tables.

20

5

10